Daily Open Source Infrastructure Report
26 April 2012

Top Stories

- Four associates of a New York businessman convicted in a $400 million Ponzi scheme were arrested on charges they pocketed nearly $38 million in commissions for their role in the fraud. – *Associated Press* (See item **17**)
- A cruise industry group announced new safety policies in response to the January 13 wreck of the Costa Concordia that killed 32 people. – *Miami Herald* (See item **24**)
- At least one major South Korean retailer suspended the sale of U.S. beef after authorities confirmed a case of mad cow disease in a dairy cow in California. – *CNN* (See item **28**)
- A group called the Threateners, which claimed responsibility for more than 100 bomb threats that caused dozens of evacuations at the University of Pittsburgh over several weeks, announced its campaign has ended. – *New York Times* (See item **40**)
- Symantec discovered new forms of Java malware that infect Mac and Windows computers. Both forms can launch a trojan that can trigger a backdoor on the computer, allowing unauthenticated access. – *Threatpost* (See item **55**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *April 25, U.S. Environmental Protection Agency* – (New Jersey) **Hess Corporation to install $45 million in pollution controls and pay $850,000 penalty to resolve Clean Air Act violations at New Jersey refinery.** The U.S. Environmental Protection Agency (EPA) and the U.S. Department of Justice announced April 25 Hess Corporation agreed to pay an $850,000 civil penalty and spend more than $45 million in new pollution controls to resolve Clean Air Act violations at its Port Reading, New Jersey refinery. Once fully implemented, the controls required by the settlement are estimated to reduce emissions of nitrogen oxide (NOx) by 181 tons per year and result in additional reductions of volatile organic compounds (VOCs). High concentrations of NOx and VOCs, key pollutants emitted from refineries, can have adverse impacts on human health, including contributing to childhood asthma, and are significant contributors to smog. The settlement requires new and upgraded pollution controls, more stringent emission limits, and aggressive monitoring, leak-detection, and repair practices to reduce emissions from refinery equipment and processing units. The state of New Jersey actively participated in the settlement with Hess and will receive half of the civil penalty.
   Source: http://yosemite.epa.gov/opa/admpress.nsf/0/365a8b086ff5958b852579eb004c6bcf?OpenDocument

2. *April 25, Indianapolis Star* – (Indiana) **About 17,000 lose power on Westside due to substation problem.** Approximately 17,000 westside and northwestside Indianapolis residents were without power April 25 because of an issue at an Indianapolis Power and Light (IPL) substation in that area. IPL workers were switching customers to other circuits and anticipated that all power would be restored around 11 a.m., an IPL spokeswoman said. Crews were also working to determine what had occurred at the affected substation and make necessary repairs, she said. About 110 customers remained without power as of 10:15 a.m.
   Source: http://www.indystar.com/article/20120425/LOCAL/204250363/IPL-restores-power-most-Westside-customers?odyssey=tab|topnews|text|News

3. *April 25, Associated Press* – (Wyoming) **Chesapeake gas well failure prompts evacuation near Douglas.** Several dozen residents near Douglas, Wyoming, were evacuated April 24 because of a problem at a natural gas well. The Glenrock Bird reported large amounts of gas were coming out of the ground late April 24, but the cause was not immediately clear. The owner of the well, Chesapeake Energy, said there was a "well control incident" but had not released any details as of the morning of April 25. A Converse County sheriff's dispatcher said residents of a subdivision were told about the problem and given the option to stay or evacuate. Over 50 of the nearly 400 residents left their homes. Residents told KCWY 13 Casper the sound of escaping

gas could be heard 6 miles away.
Source: http://fuelfix.com/blog/2012/04/25/chesapeake-gas-well-failure-prompts-evacuation-near-douglas/

4. *April 24, U.S. Department of Labor* – (Texas) **US Department of Labor's OSHA cites Pearsall, Texas, oil and gas services company for serious violations following explosion that injured 3 workers.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited High Roller Wells Pearsall SWD No. 1 Ltd. for 10 serious safety violations following an explosion and fire that injured 3 workers at the company's Pearsall, Texas work site, said an April 24 new release. The company disposes of hydraulic fracturing fluid and employs about 34 workers. At the time of the incident, employees were injecting wastewater underground that was left over from hydraulic fracturing and drilling operations. The violations include failing to: ensure workers were provided with fall protection while working on the tops of tanks; ensure equipment and electrical wiring were rated for the environment in which they were being used; take necessary precautions to prevent possible ignition sources such as sparks or static electricity; conduct a workplace hazard assessment to determine the appropriate personal protective equipment needed; ensure there was an emergency action plan in place; and provide an eyewash station for employees working around acids. Proposed penalties total $46,200.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22227

5. *April 24, U.S. Department of Labor* – (Wisconsin) **US Department of Labor's OSHA issues 15 safety violations for workplace hazards to Midwest Biofuel in Clinton, Wis., following complaint inspection.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Midwest Biofuel LLC with 15 safety and health violations, including a repeat violation for failing to provide an eye wash station, according to an April 24 news release. A complaint prompted an October 26, 2011 inspection at the organic chemical manufacturer's facility in Clinton, Wisconsin. Proposed fines total $46,200. The company was cited with 12 serious violations for failing to: use proper electrical equipment in the control room; correct deficiencies of its hazard analysis and operating procedures; investigate chemical releases; train workers engaged in chemical hazard clean-up operations; provide material safety data sheets for process chemicals; develop, implement, and train workers on the permit required confined space program; evaluate fork lift operators; develop and implement a respiratory protection program, including fit testing; and provide medical evaluations for workers required to wear respirators.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22224

For another story, see item **22**

[Return to top]

Chemical Industry Sector

6. *April 25, just-style.com* – (National; International) **New U.S. rules against harmful chemicals in dyes.** The U.S. Environmental Protection Agency (EPA) has asked all U.S.-based clothing and apparel manufacturers to report the new use of possibly harmful chemicals found in textile pigments and dyes, just-style.com reported April 25. The chemicals, which also have other industrial applications, include polybrominated diphenylethers, benzidine dyes, and hexabromocyclododecane. "Although a number of these chemicals are no longer manufactured or used in the United States, they can still be imported in consumer goods or for use in products," an EPA spokesman said. The new rules are outlined under the Toxic Substances Control Act. They require any person or company to notify the EPA 90 days before they manufacture, import, or process any of the chemicals specified, so the EPA can evaluate the chemicals and decide if they are safe. If the action is warranted, the EPA retains the right to prohibit certain new uses of the named chemicals.
   Source: http://www.just-style.com/news/new-rules-against-harmful-chemicals-found-in-dyes_id114159.aspx

7. *April 24, KGET 17 Bakersfield* – (California) **Report: Crop dusting company violated several codes.** A new report shows a Bakersfield, California crop dusting company violated several codes when one of its planes accidentally sprayed a school bus with pesticide in March. The report, released April 24, shows Inland Crop Dusters did not meet state regulations requiring chemicals to be used in a careful and effective manner. Several of the 29 kids on the bus were sickened when it was sprayed near Shafter, California. All of the children and the bus driver were decontaminated on site. The Kern County Agriculture Department is reportedly considering action against the crop dusting company.
   Source: http://www.kget.com/news/local/story/Report-Cropdusting-company-violated-several-codes/eTmndxpT90qx8QOyF5Ml-A.cspx

For more stories, see items **1**, **4**, **5**, and **32**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *April 25, RTT News* – (Pennsylvania) **PPL says Susquehanna addressing recurrence of turbine blade cracks.** According to RTT News April 25, PPL Corp. announced a planned follow-up inspection of the Unit 1 main turbine at the company's Susquehanna nuclear power plant in Salem Township, Pennsylvania, showed indications of cracks in blades that are similar to, but less extensive than, damage discovered and repaired in 2011. PPL said it will replace one row of blades on the Unit 1 turbine during the current refueling and maintenance outage and decided as a precaution to shut down the Unit 2 reactor and inspect its main turbine after the Unit 1 outage is completed. The company noted the Unit 2 outage will be scheduled after Unit 1 resumes generating electricity. The turbine blade replacement on Unit 1 will have a minimal effect on the

duration of the current outage, which began March 31 and was expected to continue into mid-May.
Source: http://www.nucpros.com/content/ppl-says-susquehanna-addressing-recurrence-turbine-blade-cracks

9. *April 24, San Luis Obispo Tribune News* – (California) **Diablo Canyon nearly idle after jellyfish-like creatures cause clog.** Diablo Canyon nuclear power plant in Avila Beach, California, was nearly idle April 24 from the combination of 1 reactor shut down for refueling and the other operating at only 15 percent capacity due to an influx of small jellyfish-like animals clogging the facility's cooling water intake structure. Plant operators reduced power on the operating reactor when large numbers of salp entered the intake structure, a plant spokesman said. "We will not increase power until intake conditions improve," he said. The other reactor was shut down earlier the week of April 23 for a planned refueling outage.
Source: http://www.sanluisobispo.com/2012/04/24/2041453/diablo-canyon-nuclear-reactor.html

10. *April 24, United Press International* – (International) **Wells to be built near damaged reactors.** Tokyo Electric Power Co. (TEPCO) said it will build wells to redirect groundwater away Japan's Fukushima No. 1 nuclear plant, United Press International reported April 24. Groundwater has been mixing with highly radioactive cooling water at the plant, increasing the amount of contaminated water at the complex, Kyodo News reported. TEPCO said the wells will direct about half of the groundwater into the Pacific Ocean before all of it goes into the reactor buildings and elsewhere. The groundwater will then be tested for radioactivity levels before being released into the ocean. The wells will likely become operational in September or October.
Source: http://www.upi.com/Top_News/World-News/2012/04/24/Wells-to-be-built-near-damaged-reactors/UPI-29881335292137/

[Return to top]

Critical Manufacturing Sector

11. *April 24, U.S. Consumer Product Safety Commission* – (National) **Gem Sensors recalls pressure transducers used in fire pump controllers due to risk of failure in a fire.** The U.S. Consumer Product Safety Commission, in cooperation with Gems Sensors, April 24 announced a voluntary recall of about 25,000 Gems 3100 pressure detectors/transducers. The transducer can fail to accurately detect water pressure in a fire suppression sprinkler system. This could cause the sprinkler system to fail to activate and pump water to the sprinklers in the event of a fire. Owners were advised to contact Gems to receive enhanced twice monthly inspection instructions and information about a free replacement transducer, when warranted.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12156.html

For another story, see item **13**

[Return to top]

Defense Industrial Base Sector

12. *April 25, Associated Press* – (New Jersey) **2 charged in NJ in military tech smuggling scheme.** Two Taiwanese nationals charged with trying to smuggle U.S. military hardware to China made their first court appearance in Newark, New Jersey, the Associated Press reported April 25. The two have been jailed since early March after being arrested and charged with selling a kilogram of methamphetamine to undercover agents. In new charges announced April 25, they are accused of conspiring to purchase drones, stealth technology, and anti-aircraft systems on behalf of buyers they said were connected to the Chinese government. Both appeared in federal court, but did not enter pleas. The two face up to 5 years for violating arms export laws, and up to life in prison for two drug counts.
Source: http://www.newswest9.com/story/17738933/2-charged-in-nj-in-military-tech-smuggling-scheme

13. *April 24, WFTS 29 Tampa* – (Florida) **Fire breaks out at Lockheed Martin in Oldsmar.** A three-alarm fire broke out at a Lockheed Martin plant in Oldsmar, Florida, April 24. Pinellas County Fire Rescue officials said the fire was contained to the roof, and crews extinguished the fire quickly. Approximately 640 employees manufacture and assemble military and commercial products at the facility. The employees were evacuated, and remained in an auditorium and a cafeteria until HAZMAT teams could give the all-clear.
Source: http://www.abcactionnews.com/dpp/news/region_north_pinellas/oldsmar/fire-breaks-out-at-lockheed-martin-in-oldsmar

For another story, see item **48**

[Return to top]

Banking and Finance Sector

14. *April 25, U.S. Securities and Exchange Commission* – (New York; National) **Attorney, Wall Street trader, and middleman settle SEC charges in $32 million insider trading case.** The U.S. Securities and Exchange Commission (SEC) April 25 announced a settlement in a $32 million insider trading case filed by the agency in 2011 against a corporate attorney and a Wall Street trader. The SEC alleged the insider trading occurred in advance of at least 11 merger and acquisition announcements involving clients of the law firm where the attorney worked. He and the trader were linked through a mutual friend, who acted as a middleman to facilitate the illegal tips and trades. The lawyer and trader used public telephones and prepaid disposable mobile phones to communicate with the accomplice in an effort to avoid detection.
Source: http://www.sec.gov/news/press/2012/2012-77.htm

15. *April 25, Financial Industry Regulatory Authority* – (Texas; National) **FINRA hearing officer expels Pinnacle Partners Financial Corp. and bars president for fraud.** A Financial Industry Regulatory Authority (FINRA) hearing officer expelled Pinnacle Partners Financial, Corp., a broker-dealer based in San Antonio and barred its president

for fraudulent sales of oil and gas private placements and unregistered securities, according to an April 25 press release. In addition, the president was found to have used customer funds for personal and business expenses. The hearing officer found that from August 2008 to March 2011, Pinnacle and its president operated a boiler room in which about 10 brokers placed thousands of cold calls on a weekly basis to solicit investments in oil and gas drilling joint ventures the president owned or controlled. They raised more than $10 million from more than 100 investors, diverting some customer funds for unrelated business and personal expenses. The hearing officer also found Pinnacle and its president included many misrepresentations and omissions in investment summaries for 11 private placement offerings, including grossly inflated natural gas prices, projected natural gas reserves, estimated gross returns, and estimated monthly cash flows.
Source:
http://www.finra.org/Newsroom/NewsReleases/2012/P126075?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+FINRANews+(FINRA+News)&utm_content=Google+Reader

16. *April 25, Krebs on Security* – (California) **Skimtacular: All-in-one ATM skimmer.** A security researcher recently received information from a law enforcement source in the California area about a recent ATM skimmer attack that showcased a well-designed and stealthy all-in-one skimmer, Krebs on Security reported April 25. The skimmer was recovered by a customer at a bank in the San Fernando Valley, who called the cops upon her discovery. Police in the region still have no leads on who might have placed the device. The numeral "5â□³ engraved in the upper right portion of the skimmer suggests it was one in a series of fraud devices produced by the skimmer maker. The skimmer appears to be powered by a phone battery that connects to the card reader device and to the circuit board for a video camera. Flip the device around, and there is a tiny pinhole where the attached camera peers through the skimmer front to capture timestamped footage of victims entering their PINs.
Source: http://krebsonsecurity.com/2012/04/skimtacular-all-in-one-atm-skimmer/

17. *April 25, Associated Press* – (New York; Florida) **NY, Fla. associates of Ponzi schemer arrested.** Four associates of a New York businessman convicted in a $400 million Ponzi scheme were arrested April 25 on charges they pocketed nearly $38 million in commissions for their efforts in advancing the fraud, federal prosecutors said. Three of the suspects were arrested without incident in New York and a fourth was taken into custody in Florida, an FBI spokesman said. The four were account representatives of Hauppauge, New York-based Agape World Inc. and Agape Merchant Advance (AMA), according to a criminal complaint. The two investment companies were run by a man who pleaded guilty to mail and wire fraud charges in a scheme that bilked more than 4,000 investors in a $400 million Ponzi scheme. The scheme targeted mainly blue-collar workers. The complaint unsealed April 25 alleges the four pocketed huge commissions for assisting the man and Agape in running the scheme. Agape promised huge returns on investments, which were to be used only to fund specific, short-term secured bridge loans to commercial borrowers or to make short-term loans to small businesses, prosecutors said. They said the defendants knew Agape and AMA did not produce or earn rates of return that could support the

exorbitant returns promised to investors, but continued to solicit money from investors. Prosecutors said that the defendants learned in November 2008 that all of Agape's 2007 bridge loans were in default or on extension, but failed to disclose that information to existing or new investors.
Source: http://www.newswest9.com/story/17737364/fbi-arrests-ny-fla-associates-of-ponzi-schemer

18. *April 24, Reuters* – (Connecticut; International) **Fugitive Swiss bank Wegelin forfeits $16 mln.** Wegelin & Co, the oldest Swiss private bank, has forfeited more than $16 million held in a UBS AG account, after becoming the first overseas bank indicted in the United States for allegedly helping U.S. taxpayers evade taxes. In an order made public April 24, a U.S. district judge in New York entered the forfeiture order, covering money seized from a U.S. correspondent account held at UBS in Stamford, Connecticut. U.S. prosecutors accused Wegelin February 2 of helping clients hide more than $1.2 billion in offshore bank accounts. They said the tax fraud conspiracy ran from 2002 and 2011, and involved more than 100 U.S. taxpayers. A U.S. attorney in New York said the forfeited funds will be deposited with the U.S. Treasury. A U.S. district judge declared Wegelin a fugitive February 10 after it failed to answer the criminal charge. Wegelin has no branches outside Switzerland, and had followed the common industry practice of using correspondent banking services to handle money for U.S. clients.
Source: http://www.reuters.com/article/2012/04/24/wegelin-idUSL2E8FOJAI20120424

19. *April 24, U.S. Securities and Exchange Commission* – (National) **H&R Block subsidiary agrees to pay $28.2 million to settle SEC charges related to subprime mortgage investments.** The U.S. Securities and Exchange Commission (SEC) April 24 charged H&R Block subsidiary Option One Mortgage Corporation with misleading investors in offerings of subprime residential mortgage-backed securities (RMBS) by failing to disclose its financial condition was significantly deteriorating. Option One, which is now known as Sand Canyon Corporation, agreed to pay $28.2 million to settle the SEC's charges. The SEC alleges Option One promised investors in more than $4 billion worth of RMBS offerings that it sponsored in early 2007 that it would repurchase or replace mortgages that breached representations and warranties. However, Option One did not tell investors about its deteriorating financial condition and that it could not meet its repurchase obligations on its own. According to the SEC's complaint filed in California, Option One was one of the nation's largest subprime mortgage lenders with originations of $40 billion in its 2006 fiscal year. When the subprime mortgage market started to decline in the summer of 2006, Option One experienced a decline in revenues and significant losses, and faced hundreds of millions of dollars in margin calls from creditors. At the time, Option One needed H&R Block, through a subsidiary, to provide it with financing under a line of credit to meet its margin calls and repurchase obligations. However, Block was under no obligation to provide that funding. Option One did not disclose this information to investors. The SEC further alleges Block never guaranteed Option One's loan repurchase obligations, and that Option One's mounting losses threatened Block's credit rating at a time when Block was negotiating a sale of Option One.
Source: http://www.sec.gov/news/press/2012/2012-76.htm

20. *April 24, Federal Bureau of Investigation* – (Oregon) **Willamette Development Services executive's wife indicted for investment fraud scheme.** The spouse of the former chief executive officer (CEO) of Willamette Development Services LLC (WDS), was arraigned in federal court April 23. She was added as a defendant to an indictment charging her husband, the former investment relations manager for WDS, and the WDS Corporation with securities fraud, mail and wire fraud, and money laundering. The 22-count superseding indictment alleges she committed these offenses as an executive with Witham Investments LLC. The indictment also alleges the WDS CEO committed bank fraud and bankruptcy fraud. The indictment alleges that from April 2006 through January 2008, through misrepresentations by the CEO and investment relations manager, WDS obtained $5,285,300 from investors for the purpose of developing at least 10 real estate projects. The indictment also alleges WDS incurred $10,795,200 of additional indebtedness from lenders. By January of 2008, none of the projects were completed and WDS was insolvent. The investors lost their entire investment. Secured lenders recovered portions of their loans through foreclosures. The indictment alleges that the CEO lied about his background and prior experience. He and the investment relations manager are also alleged to have told investors that their money would be placed in a holding account until certain financial goals were reached. Investors were also told their money would be used for specific projects, but in fact the funds were allegedly diverted to non-project purposes without investor consent. The indictment also alleges the CEO's wife laundered money through Witham Investments.
    Source: http://www.loansafe.org/willamette-development-services-executives-wife-indicted-for-investment-fraud-scheme

21. *April 24, KCBS 2 Los Angeles; KCAL 9 Los Angeles* – (California) **Investigators link 'Snowboarder Bandit' to another bank heist in Palm Springs.** Authorities linked a man known as the "Snowboarder Bandit" to a bank heist in Palm Springs, California, KCBS 2 Los Angeles and KCAL 9 Los Angeles reported April 24. The bandit, who is on the FBI's most wanted list of bank robbers, is now connected to 11 bank holdups in southern California. He is suspected of holding up a BBVA Compass branch April 20, an Orange County Sheriff's Department spokesman said. After reviewing surveillance footage, investigators April 24 determined it was the Snowboarder Bandit, an FBI special agent said. Authorities believe it was the first time since he first began targeting banks in December 2011 that the suspect has ventured out of Orange County to commit a heist. A composite sketch of the suspect was released April 23. Authorities said that before the Palm Springs robbery, it had been just over a month since the Snowboarder Bandit had hit. The FBI said that someone inside of a Wells Fargo branch in Irvine recognized the snowboarder bandit April 19. He got just inside, inquired about a safe deposit box, and then quickly left.
    Source: http://losangeles.cbslocal.com/2012/04/24/investigators-link-snowboarder-bandit-to-another-bank-heist-in-palm-springs/

[Return to top]

Transportation Sector

22. *April 25, Associated Press* – (Iowa) **Crew fatigue cited in fatal train crash.** April 24, the National Transportation Safety Board (NTSB) said crew fatigue is the probable cause of a deadly train collision in southwest Iowa. A BNSF Railway coal train slammed into a standing BNSF train near Red Oak April 17, 2011. The engineer and conductor on the coal train died. The transportation board said both members of the crew fell asleep and failed to comply with a signal requiring them to operate at a restricted speed and stop short of the standing train. The NTSB chairwoman said the investigation draws attention to the dangers of human fatigue. The board said other factors contributed to the accident, including the absence of a system that identifies the rear of a train and stops the approaching train if a safe braking profile is exceeded.
Source: http://www.omaha.com/article/20120425/NEWS01/120429866/0

23. *April 25, Associated Press* – (New York) **Fla.-bound JetBlue aircraft makes emergency landing at suburban NY airport after bird strike.** JetBlue Flight 571, bound for West Palm Beach, Florida, made an emergency landing at Westchester County Airport in White Plains, New York, April 24, shortly after hitting birds upon takeoff. A Federal Aviation Administration spokesman said the flight, carrying 54 passengers, returned to the airport and landed safely. A JetBlue spokeswoman said initial reports indicated no damage to the plane.
Source: http://www.washingtonpost.com/lifestyle/travel/fla-bound-jetblue-aircraft-makes-emergency-landing-at-suburban-ny-airport-after-bird-strike/2012/04/25/gIQAMuiigT_story.html

24. *April 25, Miami Herald* – (International) **Cruise industry responds to fatal Costa Concordia wreck with new safety rules.** In response to the January 13 wreck of the Costa Concordia cruise liner that killed 32 people, the organization that represents the cruise industry announced new safety policies. The rules were issued April 24 by the Cruise Lines International Association and European Cruise Council. They include: having more lifejackets aboard ships than required by law; limiting access to a ship's bridge at potentially dangerous times; and requiring cruise ship routes to be planned in advance and shared with all members of the bridge team. All policies were put into effect immediately. Two rules were directly related to errors believed to have led to the Concordia grounding and capsizing. The ship's captain is accused of taking the ship on an unauthorized path too close to the Italian island of Giglio while he was reportedly distracted by guests on the bridge. The captain is under house arrest and faces charges that include manslaughter and causing a shipwreck.
Source: http://www.palmbeachpost.com/accent/travel/cruise-industry-responds-to-fatal-costa-concordia-wreck-2323979.html

25. *April 25, Muncie Star Press* – (Indiana) **Muncie train fire stops up traffic.** A Norfolk Southern train hauling 104 cars came to an emergency stop in Muncie, Indiana, after witnesses saw flames shooting from one of the locomotive's engines April 24. The Elkhart-bound train was stopped at the busy Tillotson Avenue crossing on the city's west side, according to a Norfolk Southern spokesman. After the train was flagged down and came to a stop, its engineer and conductor evacuated and contacted local

emergency responders. The train was able to continue on to Elkhart with its other two engines about 2 hours later. There were no hazardous materials spilled. The stopped train — which was hauling 39 loaded and 65 empty cars — was also responsible for blocking morning traffic at the White River Boulevard, Kilgore Avenue, and Nichols Street crossings for more than 1 hour. A train official at the scene said the fire could possibly be traced to an oil line that came loose or broke, causing the oil to ignite.
Source: http://www.indystar.com/article/20120425/LOCAL/204250328/Muncie-train-fire-stops-up-traffic

For more stories, see items **7**, **31**, and **60**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

26. *April 25, Food Safety News* – (Colorado) **Colorado changes its cantaloupe growing practices.** The few Colorado farmers who grow the same brand of cantaloupe implicated in the Listeria outbreak in 2011 — the most deadly outbreak of food-borne illness in the U.S. in decades — are falling into line with growing and packing reforms that originated in California, Food Safety News reported April 25. Colorado's commission of agriculture enlisted Colorado's growers who want to carry on the "Rocky Ford" brand of cantaloupes into a new $150,000 state program. The money will go for enforcement and marketing. Colorado cantaloupe growers will accept twice-a-year safety audits by state agricultural inspectors. Colorado State University was also working with growers to make sure cleaning and cooling practices do not bring about the sort of Listeria growth that went on at Jensen Farms in 2011. The Food and Drug Administration said both equipment and cantaloupes in Jensen Farms' packing shed were contaminated with Listeria. The firm was blamed for a Listeria outbreak that sickened at least 146 in 28 states. There were 36 known deaths. Other safety steps included: requiring forced air cooling to reduce the field temperature of a harvested cantaloupe that might be 90 degrees or higher down to 40 degrees inside of 3 hours; switching from a sanitizing pool to a rapid pass-through system to keep chlorination rinse moving; starting a "seed-to-store" tracking system to isolate problems down to the box, instituting a system to make "Rocky Ford" cantaloupes traceable by to the farm where they were grown with a Smartphone code; and requiring growers to attend training and agricultural practices meetings.
Source: http://www.foodsafetynews.com/2012/04/colorado-changes-its-cantaloupe-growing-practices/

27. *April 25, WMUR 9 Manchester* – (New Hampshire) **Redhook employee dies after keg explodes.** An employee was killed when a keg exploded at the Redhook Brewery in

Portsmouth, New Hampshire, April 24. Fire officials said the man was pressuring kegs with air as part of a cleaning process when a keg exploded into two pieces. The man was hit in his chest and head. When crews arrived, according to fire officials, the man was weak and barely had a pulse before he went into cardiac arrest. He was taken to a hospital, where he later died. Investigators with the U.S. Occupational Safety and Health Administration were called to look into the incident. Fire officials described it as an industrial accident and said the brewery had a strong safety record. Redhook's president of commercial operations said all nonessential operations at the brewery were shut down while it investigates what happened.
Source: http://www.wmur.com/r/30946163/detail.html

28. *April 25, CNN* – (National; International) **S. Korea curbs U.S. beef sales after confirmation of mad cow disease.** At least one major South Korean retailer suspended the sale of U.S. beef after authorities confirmed a case of bovine spongiform encephalopathy (BSE), sometimes called "mad cow disease," in a dairy cow in central California, CNN reported April 25. Public health officials in the United States said the risk to the public was extremely low, and residents do not need to take any specific precautions. However, in South Korea, one of the largest importers of U.S. beef, the discovery was enough to prompt retailer LotteMart to remove American beef from store shelves. The South Korean government said it will step up checks on U.S. beef imports — but not halt them for now. In 2010, South Korea imported 125,000 tons of U.S. beef, a 97 percent increase from the year before, the U.S. Department of Agriculture said. The carcass was at a Baker Commodities Inc. rendering facility in Hanford, California, said the company's executive vice president. The company renders animal byproducts and had randomly selected the animal for testing April 18, he said. The sample was sent to the University of California, Davis for initial testing, which came back inconclusive. It was then sent to the U.S. Department of Agriculture's laboratory in Ames, Iowa, where it tested positive, the agency said. The carcass was in quarantine April 24. BSE is usually transmitted between cows through the practice of recycling bovine carcasses for meat and bone meal protein, which is fed to other cattle. In this case, the USDA reports it was a rare form of BSE not likely carried by contaminated feed. The Centers for Disease Control and Prevention reported the odds of a person contracting mad cow disease, even after consuming contaminated products, are less than 1 in 10 billion.
Source: http://www.cnn.com/2012/04/25/health/california-mad-cow/index.html

29. *April 25, Talladega Daily Home* – (Alabama) **Tons of feed corn stolen from Koch.** Police were investigating the theft of $175,000 worth of feed corn from the Koch Foods feed mill in Talladega, Alabama, according to a police official, the Talladega Daily Home reported April 25. The thefts appeared to have taken place between December 1, 2011, and April 23. At least some of the suspects involved would be Koch employees, the official said. The official contacted federal authorities for advice on how to proceed. It was not immediately clear whether or not the federal government might take over the case entirely.
Source: http://www.dailyhome.com/view/full_story/18347463/article-Tons-of-feed-corn-stolen-from-Koch?instance=home_news_bullet

30. *April 24, Lakeland Ledger* – (National) **OJ imports to U.S. fall 37% in February.** Orange juice imports to the United States fell 37 percent in February, the first sign a federal testing program barring OJ shipments tainted with an illegal fungicide, carbendazim, is having an impact on domestic supplies, the Lakeland Ledger reported April 24. However, the short-term impact of lower OJ supplies on farm and retail prices is probably offset by diminished OJ sales, also stemming from the bad news about carbendazim, said a citrus industry economist at the University of Florida in Gainesville. If the Florida citrus industry can not revive consumer demand, the OJ sales slump will continue over the long term, depressing farm prices, he added. The Florida Department of Citrus the week of April 16 reported OJ imports in February had fallen to 15.9 million gallons, down from 25.3 million gallons a year earlier. Imports from Brazil, which normally accounts for about half the annual total, fell to zero from 7.5 million gallons in February 2011. The U.S. Food and Drug Administration began testing OJ imports for carbendazim in January after the two largest OJ brands, Tropicana and Minute Maid, reported some of their products contained traces of the fungicide. The products were blended with imported OJ, primarily from Brazil, which appears to be the source of the contamination.
Source:
http://www.theledger.com/article/20120424/NEWS/120429574/1178?Title=OJ-Imports-to-U-S-Fall-37-in-February-&tc=ar

For another story, see item **32**

[Return to top]

Water Sector

31. *April 25, WJW 8 Cleveland* – (Ohio) **Water main break closes road; boil alert issued.** Pearl Road at Albion Road remained closed after a large water main break April 25 that closed Strongsville, Ohio, city schools and forced the Cleveland Division of Water to issue a boil alert. Officials said crews determined after a few hours that the damaged pipe was a 30-inch main. Water was seen shooting 4 to 5 feet in the air and rushing down Pearl Road into Mill Stream Run Reservation. A large sinkhole developed and most of the roadway buckled. The Cleveland Water Department said it would be 3 to 5 days before the road was completely reopened, but they planned on having certain lanes open by the afternoon. The high school, police station, and recreation center did not have water April 25.
Source: http://fox8.com/2012/04/25/water-main-break-shuts-down-part-of-pearl-road/

32. *April 24, GateHouse News Service* – (Illinois) **Truck towing herbicide tank tips over, spills into Prairie Creek.** An agricultural spreader containing about 1,200 gallons of herbicide fell into Prairie Creek in Tazewell County, Illinois, April 24. The spreader being pulled by a truck tipped over into the creek after hitting a guard rail, according to a preliminary report by the Illinois Environmental Protection Agency (IEPA). A strong chemical odor was present about 1,000 feet from the area. An unknown amount of the herbicide, as well as oil and diesel fuel from the vehicle, leaked into the water, according to a news release by the Morton Fire Department chief. Two officials on the

scene reported a large fish kill 1 mile downstream from the spill site, said an IEPA spokeswoman. Crews were working to dam the creek and prevent further contamination. A private environmental consultant was hired to design and implement a plan to minimize the effects and prevent any further damage from the accident.
Source: http://www.pjstar.com/news/x513713663/Truck-towing-herbicide-filled-tank-tips-over-spills-into-Prairie-Creek

33. *April 24, Associated Press* – (California) **Marin County sanitary district agrees to $1.5M in fines, other charges in sewage spills.** A Marin County, California sanitary district agreed to pay more than $1.5 million in fines and other charges in connection with sewage spills that released more than 3 million gallons of wastewater, the Associated Press reported April 24. The agreement between the Ross Valley Sanitary District and California state water regulators calls for the district to pay more than $800,000 in fines. The rest of the money will go towards improving sewer infrastructure and improving wildlife habitat. The bulk of the wastewater was released in two large spills in December 2010. The water district blamed the spills on a south San Francisco construction company and is suing the firm, however, state water officials said negligence by water district staff contributed to the size of the first set of spills.
Source:
http://www.therepublic.com/view/story/ee0d55bdc19f41e0b1ad5b68af3016e0/CA--Wastewater-Spill/

34. *April 24, WJW 8 Cleveland* – (Ohio) **Fish kill could turn into criminal investigation.** The East Branch of the Rocky River in Strongsville, Ohio, was the site of an investigation into a massive fish kill, WJW 8 Cleveland reported April 24. "Just over 28,000 wild animals have been killed. A majority of those are minnows that were in the waterway, darters and white suckers," said an investigator with the Ohio Department of Natural Resources (ODNR). He said the fish were reported dead April 22. "It may turn into a criminal investigation. At this point, we are trying to figure out the source so we can figure out if someone has culpability. If they threw something into a storm sewer or tributary," he said. The fish kill encompasses a 3-mile stretch of Rocky River. April 24, crews from the Northeast Ohio Regional Sewer District tested the river waters for any toxic pollutants. The ODNR said the kill area ran from the Mill Stream Run Reservation in the Cleveland Metroparks to Wallace Lake in Berea. At this point, they said it appeared to be contained but still have no idea what caused it.
Source: http://fox8.com/2012/04/24/fish-kill-could-turn-into-criminal-investigation/

For another story, see item **57**

[Return to top]

Public Health and Healthcare Sector

35. *April 25, Wichita Falls Times Record News* – (Texas) **Medical records breach possible.** The 82nd Medical Group at Sheppard Air Force Base determined that 721 patients at the Sheppard Air Force Base clinic in Wichita Falls, Texas, may have had

their privacy breached after a man returned several medical documents dating from 2003 until 2007 to the base the week of April 16. According to previous reports, a Boyd resident said he and a friend found several medical documents zipped inside a garment bag that included patient names, addresses, phone numbers, Social Security numbers, and diagnoses while searching his home for personal documents in the midst of divorce proceedings with his wife. The woman served at Sheppard Air Force Base and left active duty in 2010. The documents are not full medical records, but instead consist of individual patient encounters and are equal to about 1 day's worth of filings for the Sheppard clinic, which sees about 165,000 patients each year.
Source: http://www.timesrecordnews.com/news/2012/apr/25/medical-records-breach-possible/

36. *April 24, Salem Statesman Journal* – (Oregon) **State hospital suffers data theft.** A thief stole a back pack containing patient information of about 550 current and former patients from the car of the Oregon State Hospital's chief of psychiatry, the hospital reported April 24. Patients at Salem's Oregon State Hospital received a hand-delivered letter explaining the details of an April 13 break-in of the car. The records include patients' hospital identification number, the doctor and treatment program assigned to each patient, progress notes for about 20 of those patients, and patients' dates of birth which could include health information such as the patient's diagnosis. Hospital officials think the chance is slim that the data could be used for identity theft because the Social Security numbers of the patients were not compromised and no electronic patient information was involved. The privacy breach will be investigated by the U.S. Department of Health and Human Services' Office for Civil Rights.
Source: http://www.statesmanjournal.com/article/20120425/NEWS/304250069/State-hospital-suffers-data-theft?odyssey=tab|topnews|text|News

37. *April 24, DarkReading* – (National) **Healthcare industry now sharing attack intelligence.** Large healthcare organizations and the U.S. Department of Health and Human Services (HHS) have banded together to share attack and threat intelligence in a new incident response and coordination effort established specifically for their industry. The Health Information Trust Alliance (HITRUST) announced April 24 the launch of the new HITRUST Cybersecurity Incident Response and Coordination Center as an online community for helping spot cybersecurity attacks against healthcare organizations and coordinating incident response to threats and attacks. According to a founding participant, attacks against healthcare organizations are becoming more targeted and focused, and cyber criminals are going after Web portals and healthcare applications as their point of entry, rather than the previous method of hitting the perimeter.
Source: http://www.darkreading.com/database-security/167901020/security/attacks-breaches/232900882

[Return to top]

Government Facilities Sector

38. *April 24, Myrtle Beach Sun News* – (South Carolina) **Socastee High School evacuated Tuesday after bomb threat.** Socastee High School officials in Myrtle Beach, South Carolina, resumed classes about 3 and a half hours after the building was evacuated April 24 following a bomb threat found in a boys bathroom, said a Horry County Schools spokeswoman. She said students were held outside while police searched the building. Horry County police's bomb squad searched the building, a police official said. It was the 13th bomb threat made at a Horry County School in 2012, according to authorities.
Source: http://www.myrtlebeachonline.com/2012/04/24/2791421/socastee-high-school-being-evacuated.html

39. *April 24, Des Moines Register* – (Iowa) **Bomb threat forces Carlisle Middle School evacuation.** Officials evacuated Carlisle Middle School in Carlisle, Iowa, April 24 after finding a bomb threat and dismissed all district students later in the day. The Carlisle schools superintendent said a student found a message in a bathroom at the middle school. She reported it, and the school was immediately evacuated. District officials moved the students to the high school but decided to dismiss the other schools early and notified parents about the threat and the early dismissal. About 25 people were searched the school after it was evacuated.
Source: http://www.desmoinesregister.com/article/20120425/NEWS01/304250027/-1/AMES/Bomb-threat-forces-Carlisle-Middle-School-evacuation

40. *April 24, New York Times* – (Pennsylvania) **Group says it has ceased bomb threats on campus.** As students headed to final exams at the University of Pittsburgh in Pittsburgh the week of April 23, they were hoping there would be no further evacuations now that a group that claimed responsibility for more than 100 bomb threats has announced its bomb threat campaign is over, the New York Times reported April 24. Calling itself the Threateners, the group claimed responsibility for dozens of bomb threats delivered by e-mail to Pittsburgh-area news outlets since March 30. The weekend of April 21, in an open letter to the university's chancellor, the group said it would stop if the university withdrew its $50,000 reward for information leading to the arrest of the people behind the threats. In early April, on the advice of law enforcement officials, the university refused to negotiate with what appears to be the same anonymous group, university officials said. However, April 21, the offer of a reward vanished from the university's Web site. Officials said no threats have been received since April 21. Bomb-sniffing dogs had been on the scene since February 13, when the first threat was found scribbled on a wall in a women's restroom in a chemistry building. The Threateners, in an e-mail sent to the campus newspaper, the Pitt News, and addressed to the chancellor, claimed responsibility only for e-mail threats since March 30. While the bomb threats prompted some students to abandon dorms and classrooms and head home early this semester, university officials vowed to keep the campus open and operating, turning to Twitter and other social media tools to inform students of threats and when buildings were clear for them to return. Professors abandoned attendance policies and gave lectures online. Facebook pages and Google spreadsheets offered off-campus accommodations for students weary of being

evacuated. The university announced security measures would be put in place for graduation April 29.
Source: http://www.nytimes.com/2012/04/25/us/group-says-it-has-ceased-bomb-threats-at-university-of-pittsburgh.html

41. *April 24, KMOV 4 St. Louis; Associated Press* – (Missouri) **Man charged with throwing firebomb at federal building downtown.** A southwestern Illinois man was charged after he allegedly threw an explosive device at a federal building in downtown St. Louis, April 23. Prosecutors said the suspect was charged with attempted destruction of U.S. property by fire or explosion. According to the affidavit, the suspect drove up to the government building and parked his car near the security guard shack. Officials said a guard on duty saw the suspect go towards the building, then return to his vehicle and retrieve something similar to a Molotov cocktail. Investigators said a guard saw the man light the device and throw it at the building, causing a fireball that scorched the wall and sidewalk. St. Louis police officers later recovered a broken glass bottle. The building houses several government agencies, including Homeland Security, Housing and Urban Development, the U.S. Coast Guard, and the U.S. Army Corps of Engineers. If convicted, the suspect faces up to 20 years in prison and fines of up to $250,000.
Source: http://www.kmov.com/news/crime/Man-charged-with-throwing-explosive-device-at-federal-building-in-downtown-St-Louis-148752875.html

42. *April 24, WFXT 25 Boston* – (Massachusetts) **Stoughton High School student allegedly planned 'Columbine-style' attack.** A Stoughton High School student in Stoughton, Massachusetts, was being held without bail after a school administrator discovered his journal which outlined a "Columbine-style" attack, WFXT 25 Boston reported April 24. The teenager was arraigned April 20 on a multitude of charges, including causing a school disturbance, four counts of threatening to commit a crime, and a felony charge of making a terroristic threat. He appeared at a dangerousness hearing April 24. A Stoughton Police lieutenant said the teen did not have access to firearms. Based on information in the journal, police felt there was enough information to make an arrest. A reverse 9-1-1 call went out to parents of students at Stoughton High School.
Source: http://www.myfoxboston.com/dpp/news/local/stoughton-high-school-student-allegedly-planned-columbine-style-attack-20120424

43. *April 24, Cranford Chronicle* – (New Jersey) **Union County College Cranford campus clear after fourth security threat.** No dangerous materials were found during a sweep of Union County College's Cranford, New Jersey campus, April 24, after the school received its fourth threat in April. A "very vague" threat was phoned in to the school, said the school's vice president. The school's public safety department cleared the campus about an hour and a half after the threat was received. Students and faculty were notified by e-mail that security officers were sweeping the building.
Source:
http://www.nj.com/cranford/index.ssf/2012/04/union_county_college_cranford_1.html

For more stories, see items **7**, **31**, **48**, and **53**

[Return to top]

Emergency Services Sector

44. *April 24, WFAA 8 Dallas-Fort Worth; CNN* – (Texas) **Police car stolen, crashed into fence.** Police said a man hopped in a cruiser after running out of the courthouse April 24 to avoid arrest on a felony warrant in Fort Worth, Texas, stealing the car of an officer who was chasing him. Shortly after, the man crashed into an SUV and hit a fence. Police were investigating whether the officer followed proper policy in securing the cruiser.
Source: http://www.ksdk.com/news/article/317658/28/Police-car-stolen-crashed-into-fence

45. *April 24, San Bruno Patch* – (California) **County emergency services need improvement, report says.** The San Bruno Patch reported April 24 that a San Mateo County, California grand jury report has found that the county office of emergency services is still not ready to properly handle a disaster nearly 2 years after the 2010 pipeline explosion in San Bruno, California. During the explosion, the jury assembly room in the basement of the Redwood City Hall of Justice was used to coordinate the county's response to San Bruno. But the fact that hundreds of people use the room, cell phone reception is spotty and electronic equipment is antiquated means it would not be adequate to serve as an emergency operation center if another disaster struck, the grand jury concluded. Now, the county board of supervisors and the sheriff's office have 6 months to establish a fully-functioning emergency center, according to the grand jury. The county emergency services office is also being required to establish better communication with the Red Cross and follow through on improvements recommended after the San Bruno fire. Out of 13 improvements recommended in the aftermath of the explosion, the county emergency services office only followed through on 4 of them, the grand jury found.
Source: http://sanbruno.patch.com/articles/county-emergency-services-need-improvement-report-says

For more stories, see items **31** and **40**

[Return to top]

Information Technology Sector

46. *April 25, H Security* – (International) **Firefox 3.6.x reaches end of life.** The 3.6.x branch of Mozilla's Firefox Web browser reached its end of life April 24 — no further updates, including security updates and critical fixes, will be made available for the series. According to recent Platform Meeting Notes, users running Firefox 3.6.13 to 3.6.28 should have already started receiving "Major Update" prompts asking them to upgrade to the latest stable release of the browser. All of these users are advised to upgrade as soon as possible. A number of users and organizations previously stayed on the legacy branch of Firefox due to worries over Mozilla's new Rapid Release process,

which sees a new update to the browser arrive every 6 weeks. For enterprises, this meant they would not have sufficient time to test and certify any given version before the next one was released. To address these concerns, Mozilla created an Extended Support Release (ESR) of Firefox aimed at enterprises and other large organizations. Alongside the release of Firefox 12 April 24, Mozilla also updated Firefox ESR, which is currently based on Firefox 10, to version 10.0.4. The update is the first ESR release to complete the qualification phase of the ESR life cycle that is designed to ensure the quality of the release. The new ESR release fixes various bugs and closes a total of 11 security holes, including 6 critical vulnerabilities for problems related to WebGL, OpenType Sanitizer, font-rendering with airo, gfxImageSurface, IBMKeyRange, FreeType, and miscellaneous memory safety hazards.
Source: http://www.h-online.com/security/news/item/Firefox-3-6-x-reaches-end-of-life-1558484.html

47. *April 25, Wired* – (International) **Anti-viral: Facebook partners with security vendors to stop malware.** Facebook is partnering with the Internet's top security software vendors in an attempt to crack down on users sharing URLs that lead to phishing and virus-laden Web sites, the company announced April 25. Users can also get a free 6-month trial of the companies antivirus software to install on their computers. In the deal, Microsoft, McAfee, TrendMicro, Sophos, and Symantec will share with Facebook their databases of malicious URLs, adding to Facebook's own system for preventing users from sharing known links to sites that could install malware.
Source: http://www.wired.com/threatlevel/2012/04/facebook-partners-security/

48. *April 25, Help Net Security* – (International) **VMvare confirms server hypervisor source code leak.** VMware confirmed a file from the VMware ESX server hypervisor source code was leaked by a hacker that goes by the handle "Hardcore Charlie." The posted code and associated commentary dates to the 2003 to 2004 timeframe, said the director of VMware's Security Response Center. He added there is a possibility more files may be posted in the future, as the hacker claimed to have in his possession around 300 MB of VMWare source code. He said the fact the source code may have been publicly shared does not necessarily mean there is any increased risk to VMware customers. The leaked file was part of a batch of documents released by the hacker. The provenience of the leaked code has not been confirmed, but it appears to originate from the servers of the China Electronics Import & Export Corporation, which recently suffered a breach, allegedly at the hands of Hardcore Charlie. According to Threatpost, the hacker boasted of breaching many big firms in the Asia-Pacific region, and said he possesses more than a terabyte of data stolen from their servers. He also claims he and his associates still have access to the networks of some of these firms. Some documents were already leaked online, and among them are shipping documents of U.S. military transports in Afghanistan.
Source: http://www.net-security.org/secworld.php?id=12807&utm

49. *April 25, H Security* – (International) **Online forums hacked and misused on a large scale.** Online forums have, for some time, been the target of hackers who inject additional code looking for money. They steal Google traffic from the forums and

exploit this traffic via ads. Their main targets appear to be forums based on the vBulletin software. These attackers have discreet working methods. They hide their code deep in a system and ensure redirections do not attract attention. Only users who visit forum pages for the first time via a search engine are redirected to a url123.info URL. The site first displays a strange blocking alert ("Access denied") followed by arbitrary text and then loads a full-page ad by InfinityAds. The ads are probably a direct source of income for intruders even though each ad is only worth a few pennies. However, as some forum operators noted, their traffic has dropped by more than 70 percent, and the phenomenon seems widespread, so the overall yield could be considerable. Forum owners and regular forum users who access pages directly never encounter the redirection. Neither will those who try to reproduce the issue by repeatedly clicking through to the forum via Google be redirected, because a cookie already exists for the page. One way of reliably reproducing the redirection is to carry out a search with a browser in private or anonymous mode.
Source: http://www.h-online.com/security/news/item/Online-forums-hacked-and-misused-on-a-large-scale-1558917.html

50. *April 25, H Security* – (International) **Thunderbird and SeaMonkey updates arrive, close security holes.** Mozilla recently published updates to Thunderbird and SeaMonkey. The updates remedy 13 vulnerabilities in each application. Six of these are considered to be critical and originate in problems related to WebGL, OpenType Sanitizer, font-rendering with Cairo, gfxImageSurface, IBMKeyRange and miscellaneous memory-safety hazards. Four of the remaining issues are rated as "High" risk, while the three remaining bugs are "Moderate." In the release announcement for Thunderbird, the developers also remind users the legacy 3.1.x branch of the application reached its end of life and no further updates, including security updates and critical fixes, will be made available for the series.
Source: http://www.h-online.com/security/news/item/Thunderbird-and-SeaMonkey-updates-arrive-close-security-holes-1558957.html

51. *April 24, Computerworld* – (International) **Mozilla delivers silent updating with Firefox 12 release.** April 24, Mozilla released Firefox 12, patching 14 security bugs in the browser and moving it one step closer to silent updating. The latest in the line of updates that rolled off the Mozilla development line every 6 weeks since mid-2011, Firefox 12 fixed seven vulnerabilities labeled "critical," the highest threat ranking in Mozilla's four-step scoring, four bugs tagged "high," and three pegged "moderate." Mozilla also patched 19 other bugs, all critical, in the mobile edition of Firefox, which runs on the Android platform. Among the 14 desktop vulnerabilities, Mozilla patched 3 that could be used by hackers in cross-site scripting (XSS) attacks, one that applied only to Windows Vista and Windows 7 PCs with hardware acceleration disabled, and another in image rendering done by the WebGL 3D standard.
Source:
http://www.computerworld.com/s/article/9226529/Mozilla_delivers_silent_updating_with_Firefox_12_release

52. *April 24, U.S. Consumer Product Safety Commission* – (National) **Lenovo expands recall of ThinkCentre desktop computers due to fire hazard.** The U.S. Consumer

Product Safety Commission, in cooperation with Lenovo, announced a voluntary recall of about 13,000 Lenovo ThinkCentre M70z and M90z computers April 24 (50,500 were previously recalled in March). The manufacturer/importer of the product was Lenovo, of Morrisville, North Carolina. A defect in an internal component in the power supply can overheat and pose a fire hazard. Lenovo received reports of one fire incident and one smoke incident. The computers were sold online at Lenovo's Web sites, by telephone, and direct sales through Lenovo authorized distributors nationwide from May 2010 through March 2012.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12159.html

53. *April 24, Government Computer News* – (International) **FBI, working group reinforce effort to rid computers of DNSChanger.** The FBI and a working group of security experts relaunched their campaign to rid computers of the DNSChanger malware that still threatens to cut hundreds of thousands of users off from the Internet in July. The ad hoc DNSChanger Working Group has a new Web site that links to instructions on how users and organizations can find and remove DNSChanger from their machines, along with updates on the effort. The FBI also has a Web page devoted to fixing the problem. DNSChanger infected as many as 4 million computers around the world as part of an Estonia-based clickjacking scheme the FBI busted in November 2011. The malware redirected infected computers to the ring's servers, which then sent them to bogus sites, while also disabling antivirus software. After the FBI broke up the ring and arrested six of its principals, it received a court order to allow the Internet Systems Consortium to run temporary replacement DNS servers in place of the ring's servers. Otherwise, infected computers would have had their DNS requests sent to servers that were taken offline, effectively cutting them off from the Internet. The original court order was to expire in March, but the FBI obtained an extension until July 9 to allow more time to clean infected machines. Much progress has been made in ridding machines of the malware, and federal agencies have largely been cleaned of infections, but an estimated 350,000 could still be at risk. The new campaign is designed to raise awareness about the threat, so users and organizations check for the malware and remediate the problem if it is on their machines.
Source: http://gcn.com/articles/2012/04/24/dnschanger-fbi-working-group-new-campaign.aspx

54. *April 24, Threatpost* – (International) **OpenSSL releases new fix for CVE-2012-2110 ASN1 bug.** The OpenSSL developers had to re-release the fix for a serious vulnerability in the software's ASN.1 implementation that could allow an attacker to cause a denial-of-service or potentially run arbitrary code on a remote machine. The updated fix only applies to version 0.9.8v; all of the other previously affected versions are already protected with the existing patch. OpenSSL released the original advisory and fix for the CVE-2012-2110 vulnerability the week of April 16, fixing the bug in versions 0.9.8, 1.0.1a, and 1.0.0i. However, after releasing the fixes, Red Hat discovered the fix for version 0.9.8 did not completely address the vulnerability, hence the new patch. "The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other

impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key," according to the description of the bug in the National Vulnerability Database.
Source: http://threatpost.com/en_us/blogs/openssl-releases-new-fix-cve-2012-2110-asn1-bug-042412

55. *April 24, Threatpost* – (International) **New Java malware exploits both Windows and Mac users.** Symantec discovered a new form of Java malware that infects Apple and Windows machines. The company's research describes a strain of Java Applet malware that either drops a Python-based malware in Mac operating systems or an executable-form of malware in Windows computers. If opened, both forms could launch a trojan that could trigger a backdoor on the computer, regardless of the platform. The malware exploits the Oracle Java SE Remote Java Runtime Environment Code Execution Vulnerability (CVE-2012-0507) to download the malware. The post said the Mac trojan can currently only control polling times, or "how many times it gets commands from the server at certain time intervals." If enabled however, the trojan can also download files, list files and folders, open a remote shell, sleep, or upload files. The trojan for Windows can send information about the infected computer and disk, its memory usage, OS version and user name, in addition to downloading and executing files and opening shells to receive commands. The news of this malware comes after the discovery of Flashback and SabPub, two forms of malware that targeted Mac users throughout the first quarter of 2012 via another vulnerability in Java. The vulnerability CVE-2012-0507 — an older Java flaw recently blocked by Mozilla's Firefox — was used by some Flashback variants earlier in April, before being patched by Apple.
Source: http://threatpost.com/en_us/blogs/new-java-malware-exploits-both-windows-and-mac-users-042412

For another story, see item **37**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: https://www.it-isac.org

[Return to top]

Communications Sector

56. *April 25, Brattleboro Reformer* – (Vermont) **Thieves steal live telephone lines.** Police said someone cut down several telephone lines in Dover, Vermont, to steal the copper. According to the Dover police chief, at about 3 a.m. April 20 about 800 feet of cable was cut from the utility poles along North Street in the East Dover section of town. Police were first alerted to the theft after FairPoint Communications said they had received a report of an outage and discovered the missing telephone lines at the scene. The chief said he is looking into the possibility of bringing in the FBI to assist with the

case.
Source: http://www.reformer.com/localnews/ci_20473719/thieves-steal-live-telephone-lines

For more stories, see items **47**, **49**, and **51**

[Return to top]

Commercial Facilities Sector

57. *April 25, U-T San Diego* – (California) **Beaches still closed after big sewage spill.** South County, California beaches remained closed 3 weeks after a major sewage spill caused by a software malfunction and operator error at a sewage plant in San Ysidro, U-T San Diego reported April 25. At least 2 million gallons of raw sewage leaked into the Tijuana River earlier in April. Officials at the South Bay International Wastewater Treatment Plant met April 24 with the environmental groups that originally alerted the public to the incident. The groups hoped to determine when a malfunctioning pump can be turned back on and when the beaches can reopen. They also planned to discuss ways to alleviate the communication breakdown that prevented the public from knowing about the spill until more than a week after it occurred.
Source: http://www.utsandiego.com/news/2012/apr/25/tp-beaches-still-closed-after-big-sewage-spill/

58. *April 24, WBIR 10 Knoxville* – (Tennessee) **3 in hospital after Cocke Co. daycare E.coli outbreak.** Three children were sent to a hospital following an E.coli outbreak at a Newport, Tennessee daycare facility, WBIR 10 Knoxville reported April 24. According to the Tennessee Department of Health, three juveniles, all of whom attend the same daycare facility, were diagnosed with E.coli symptoms. The source of the bacteria was unknown, but managers of the facility were working with investigators. The families of all children who attend the daycare were contacted. State health department officials did not close the facility but were continuing to investigate the situation.
Source: http://www.wbir.com/news/article/217724/2/3-in-hospital-after-Cocke-Co-daycare-Ecoli-outbreak?odyssey=tab|topnews|bc|large

For more stories, see items **11**, **31**, and **53**

[Return to top]

National Monuments and Icons Sector

59. *April 25, KPHO 5 Phoenix* – (Arizona; New Mexico) **Wildfire burns 200 acres in Coronado National Forest.** A lightning-caused wildfire near Safford, Arizona, has consumed more than 200 acres in the Coronado National Forest. A Coronado National Forest spokeswoman said the Cedar Fire started April 22 in the Safford Ranger District. She said that as of the morning of April 25, 70 percent of the fire was contained, noting, however, that rough terrain made fighting the fire a challenge. The fire was

burning mostly grass and brush. There are about 20 structures are in the area, but none were in imminent danger, the spokeswoman said.
Source: http://www.kpho.com/story/17707657/blaze-continues-to-burn-in-coronado-national-forest

For another story, see item **60**

[Return to top]

Dams Sector

60. *April 25, Marietta Times* – (Ohio) **Damage at dam on Muskingum River to be repaired.** A routine inspection in February uncovered deterioration on the Muskingum River Parkway Lock and Dam No. 7 that could have caused property damage and river transportation headaches north of McConnelsville, Ohio. The offices of a state representative announced the week of April 23 that the Ohio Controlling Board had approved the release of $37,600 for repairs. An assistant park manager for multiple state parks said deterioration of sheet piling in three of the dam's cells on the western end of the 472-foot structure was detected. Within 2 weeks, the repairs were completed by pumping concrete into the gaps in the 20-foot-diameter cells. Most likely, problems would have occurred upstream from the dam, the "bank would've started caving in," the manager said, noting that could affect property and roads along the river.
Source: http://www.mariettatimes.com/page/content.detail/id/543696/Damage--at-dam-on-Muskingum-River-to--be-repaired.html?nav=5002

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer